TUTTO QUELLO CHE GLI ALTRI NON DICONO
NO PUBBLICITÀ
SOLO INFORMAZIONE E ARTICOLI
2€
n.175
HACKER JOURNAL
www.hackerjournal.it
PEER TO PEER
TUTTO IL SOFTWARE DI EMULE
TECNICHE
SQL INJECTION
IL DATABASE È NUDO
ATTUALITÀ
GUERRA
AL SOFTWARE INUTILE
INTERNET
HACKING CHALLENGER
LA SFIDA È APERTA
QUATTORD. ANNO 9 - N° 175 - 30 APRILE/13 MAGGIO 2009 - € 2,00
LINUX
OFFICE 2007
SPOSA IL PINGUINO
SECURITY
THE BOINC PROJECT
COME TI TROVO IL NOTEBOOK RUBATO
WLF PUBLISHING

Anno 9 – N.175
30 aprile/13 maggio 2009

Editore (sede legale):
WLF Publishing S.r.l.
Socio Unico Medi & Son S.r.l.
via Donatello 71
00196 Roma
Fax 063214606

Realizzazione editoriale
a cura di BMS Srl

Printing:
Roto 2000

Distributore:
M-DIS Distributore SPA
via Cazzaniga 2 - 20132 Milano

Copertina: Daniele Festa

HACKER JOURNAL
Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.

Una copia 2,00 euro

Direttore Responsabile:
Teresa Carsaniga

hack·er (hăk'∂r)
"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

editoriale

Scandalosi aggiornamenti

"La perfezione della tecnologia e la confusione degli obiettivi sembrano, a mio parere, caratterizzare la nostra epoca".
Albert Einstein

È un dato di fatto, ormai, che tramite le tecnologie legate al peer to peer si scambiano giornalmente milioni di copie di film e canzoni illegali; molti non sanno che è proprio tramite Torrent o eMule che circolano migliaia e migliaia di copie di qualsiasi genere di software.

Questa battaglia sommersa vede da un lato le software house che accusano la pirateria di metterle in crisi e dall'altra parte della barricata utenti spinti dalle motivazioni più varie: costi del software troppo elevati, royalties carissime, aggiornamenti dai costi spropositati e altro ancora.

Proprio la questione degli aggiornamenti sembrerebbe quella più spinosa: pensiamo a un programma diffuso come Word ma nella sua versione del 1995. Permetteva di scrivere libri, lettere, appunti e altro ancora. Già allora disponeva di moltissime funzioni che i più ignoravano. Purtroppo aveva anche diversi problemi di stabilità e, sui sistemi attuali, non può essere installato facilmente a causa della sua struttura. Windows Vista lo dichiara addirittura come incompatibile. Per installare Word su un computer nuovo di zecca, con Windows Vista, occorre aggiornarlo: un'operazione dal costo non indifferente. Certo, la nuova versione ha funzioni in più… che la maggior parte degli utenti, ovviamente, non sa nemmeno di avere, esattamente come per le versioni precedenti. Le cose vanno ancora peggio se si pensa a software che, sostanzialmente, non hanno avuto cambiamenti funzionali nel corso degli anni. Pensiamo ad Adobe che nel giro di poco ha rilasciato le sue CS1, CS2, CS3 e CS4, spacciando la versione 2 come un software a tutti gli effetti quando, invece, soffriva di problemi gravissimi ed è stato considerato, dagli esperti, nulla più che una versione beta della CS3. Una pratica commerciale non certo usata solo da Adobe: Microsoft l'ha ampiamente utilizzata nei passaggi da Windows 95 a Windows 98, 98 Second Edition, Millennium e XP

Ovviamente, le software house non ne hanno colpa, ci mancherebbe, loro forniscono il software così com'è. Se non funziona correttamente nessun problema. Basta chiedere, a chi ha pagato per comprarlo, di sborsare altri soldi per aggiornarlo a una versione funzionante.
Ci piacerebbe vedere le conseguenze di un simile atteggiamento anche per altri beni di consumo: la macchina non sterza se piove? Nessun problema, paghi un nuovo motore e vedrai che spettacolo.

È per questi motivi che il P2P è tanto ricco di software ed è per questi motivi che inneggiamo all'uso di software open source. Un software pulito, liberamente utilizzabile, corretto da community di liberi programmatori, in continua evoluzione e capace di dare una spinta definitiva a un mercato statico e soffocante.

The Guilty

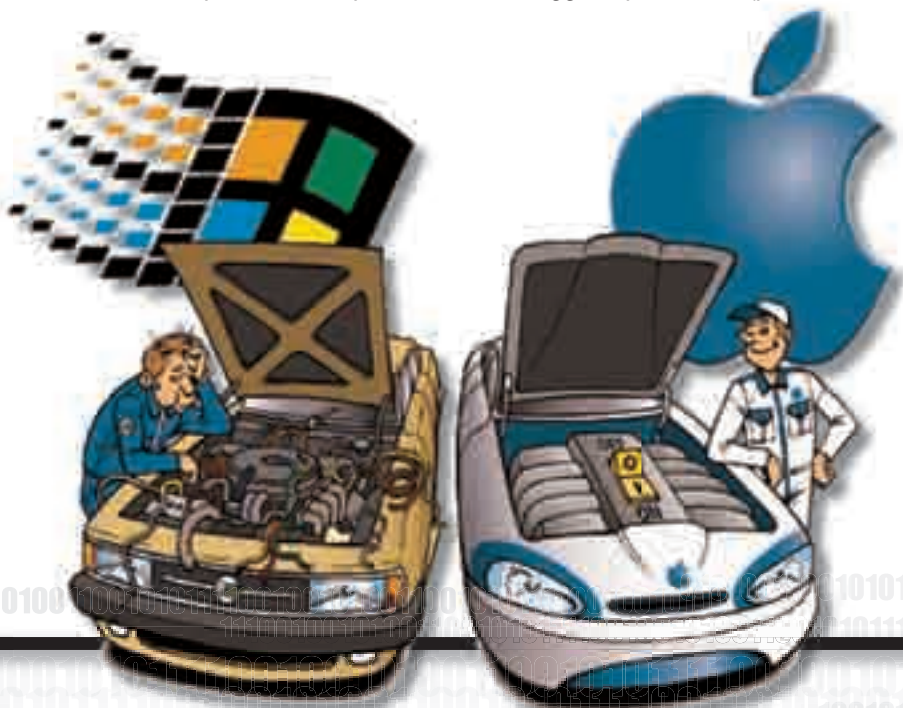
HACKER JOURNAL: INTASATE LE NOSTRE CASELLE

Diteci cosa ne pensate di HJ, siamo tutti raggiungibili via e-mail, tramite lettera o messo a cavallo... Vogliamo sapere se siete contenti, critici, incazzati o qualunque altra cosa!
Appena possiamo rispondiamo a tutti, scrivete!

redazione@hackerjournal.it

Spectrum o C64?

Era una battaglia cruenta, combattuta a suon di caratteristiche tecniche e di software che spingevano sempre oltre i limiti di ciò che si poteva fare con l'una o con l'altra macchina.
Erano anche gli anni '80, ma non è tutta storia passata. Una decina d'anni più tardi ha preso forma un'altra guerra ideologica tra utenti informatici: PC o Mac? In questo caso il mercato e le politiche aziendali hanno assegnato al PC il trono nelle camerette di molti ragazzi e negli uffici di tipo amministrativo, mentre al Mac un posto fisso in tutte le attività professionali con spiccate tendenze verso la grafica e il DTP. In tutti questi anni, Apple ha sempre combattuto per far uscire il suo Mac dalla nicchia in cui era stato posto. Per farla breve, ritocchi anche pesanti alle tecnologie e ai prezzi hanno reso i computer della mela accessibili a tutti, anche agli utenti meno esperti che preferiscono qualcosa di alternativo e semplice da usare. Almeno, è quello che traspare osservando i prezzi e le caratteristiche delle macchine di oggi, in vendita anche nei centri commerciali. Ovviamente, questo non ha fatto altro che rosicchiare la fetta del mercato di Microsoft, complici anche i ritardi nell'uscita di nuovi sistemi operativi, dei problemi che ancora li affliggono e nell'elaborata concezione delle interfacce, forse troppo difficili da usare per chi non ha mai utilizzato un computer. Fatto sta che siamo arrivati al punto che, per difendersi da Apple, la casa di Redmond ha fatto letteralmente i conti in tasca a Cupertino. Chi compra Apple, secondo Microsoft, è destinato a spendere molto di più nell'arco di vita del computer di chi compra un PC Windows, per aggiornamenti software e garanzie varie. Ad occhi poco attenti questo può anche risultare vero, o almeno plausibile. In realtà, basta spulciare un attimo i dettagli della denuncia di Microsoft per trovarne le pecche: per un Apple si conta l'acquisto di un modello top di gamma e del relativo software che invece non viene conteggiato per un PC (perché ritenuto preinstallato, ma Office preinstallato, se lo si trova, lo si paga e nemmeno poco), oppure si considerano per un Mac costi che in realtà sono del tutto opzionali, per esempio per software di cui esistono alternative free. L'analisi iniziale è stata commissionata e pagata da Microsoft all'esperto Roger Kay e non è frutto di indagini indipendenti, quindi ognuno può trarne le proprie conclusioni. La guerra, a quanto pare, continua.

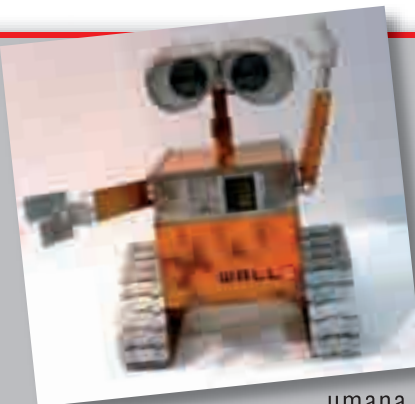
▲ ***La "lista della spesa", o meglio delle "tasse" che, secondo Microsoft, Apple impone ai propri utenti.***

PRIMAVERA TEMPO DI BLUETOOTH

Il 21 aprile scorso sono state definite le ultime specifiche universali della nuova piattaforma wireless Bluetooth: il BT 3.0. La nuova tecnologia permetterà una velocità di trasmissione di circa 480 Mbit al secondo nel raggio di 10 metri, che scenderà ad un valore di 100 Mbit al secondo nel caso di distanza superiore, fino a 100 metri. La maggiore innovazione introdotta nello standard Bluetooth 3.0 è però la piena compatibilità con il Wi-Fi 802,11 b/g, il che significa che i nuovi dispositivi saranno collegabili ai router Wi-Fi: in questo modo si abbatterà il concetto di Wireless di "serie A" e di "serie B", unificando i maggiori pregi dei due.

Mr MAC LAVORA A UN PROGETTO SEGRETO

Ogni anno, in prossimità del consueto evento Apple di giugno, si susseguono le voci di nuovi e incredibili prodotti destinati a cambiare il nostro modo di utilizzare la tecnologia. Spesso si tratta di pure invenzioni frutto della fantasia dei fans di Apple, ma qualche volta, come nel caso dell'iPhone, i prodotti della mela rappresentano davvero svolte epocali nel mondo dell'informatica. A gennaio di quest'anno la notizia che Steve Jobs, numero uno di Apple, avrebbe lasciato per sei mesi l'incarico di amministratore delegato per motivi di salute, aveva sconvolto tutti gli appassionati. In realtà pare che Jobs non sia stato con le mani in mano durante questo periodo di "malattia", ma si sia dedicato più da vicino ad alcuni " progetti segreti" tra i quali un presunto "tablet PC" a metà tra un PC e un iPhone, chiaramente multitouch. Il nuovo dispositivo, già ribattezzato dagli appassionati "iTablet", dovrebbe colmare la lacuna di Apple in un segmento di mercato, quello dei PC ultraportatili, ormai dominato dai netbook. Staremo a vedere se Jobs tirerà fuori dal suo magico cappello un nuovo prodigio oppure se si tratterà dell'ennesimo "miraggio" degli Apple-maniaci.

IL ROBOTTINO FA DA PC

La fantasia dei modder non ha confini. I più bravi riescono a nascondere un pc praticamente in qualsiasi oggetto in grado di contenere una scheda madre e qualche ventola: cassetti, quadri da appendere al muro, mattoncini lego, l'abilità degli appassionati di "personalizzazione del PC" è davvero incredibile. Tuttavia il case realizzato dai russi di www.casemods.ru supera ogni

umana immaginazione. Ispirandosi al popolarissimo film di animazione della Pixar "Wall-E", i modder sovietici hanno creato un case in cui inserire il PC che riproduce il simpaticissimo robottino del film a grandezza naturale. Il lavoro di costruzione del computer ha richiesto oltre 18 giorni di lavoro, e l'utilizzo di dispositivi ad alta precisione per realizzare i componenti in metallo ed assemblarli senza danneggiare i componenti del PC. Non sappiamo se il computer sia o meno in vendita.. ma crediamo che il prezzo supererebbe di molto i 2000 euro, scatenando un'asta selvaggia tra gli appassionati e i collezionisti.

ATTACCO A SILICON VALLEY

I film di fantascienza esagerano: ogni attacco informatico che vediamo sul grande schermo è il frutto di una mente geniale e malata in grado di convogliare la potenza di milioni di computer su un unico obiettivo per neutralizzarlo. La realtà è molto più semplice. Dei "geniali" hacker californiani hanno bloccato la connessione a Internet di centinaia di aziende della Silicon Valley con il più semplice degli attacchi: staccando i cavi! In realtà la cosa non è stata così semplice visto che i "pirati" hanno dovuto per prima cosa localizzare il punto esatto sotto cui passava la dorsale di fibra ottica che collegava la Silicon Valley al resto della rete, scavare per decine di metri e successivamente recidere i cavi. Un attacco davvero terribile che ha gettato nel panico mezza California per diversi giorni. Il lavoro di riallacciamento dei cavi in fibra ottica non è affatto semplice.

GOOGLE PUNTA SULLA VOCE, MICROSOFT SUL TATTO

Due approcci diversi allo stesso problema. È sorprendente vedere come due dei principali leader del mercato dell'informatica vedano il futuro in modo così diverso. Google infatti ha deciso di potenziare lo sviluppo di applicazioni compatibili con la tecnologia "voice search" che permette agli utenti di cercare un documento o un testo senza tastiera. Secondo Google, questo tipo di interazione renderà le ricerche velocissime e sarà possibile dialogare liberamente con il computer (o il telefonino) senza più bisogno di artifici. Di parere opposto è Microsoft, che ha deciso di abbandonare lo sviluppo di applicazioni di controllo vocale in favore del multitouch. Secondo Microsoft infatti, utilizzare le dita per impartire comandi al computer è più semplice. I sistemi di riconoscimento vocale presentano molti più margini di errore rispetto alle pellicole sensibili, rendendo il controllo vocale del computer un'attività frustrante nella maggior parte dei casi. Chi avrà ragione?

HACKER FILM FEST A MILANO

Si è tenuto a Milano lo scorso 26 marzo presso lo Spazio Anteo, l'Hacker Film Festival, rassegna cinematografica dedicata al mondo degli hacker e in particolar modo a come i mass media interpretano la figura del "pirata" informatico. La manifestazione ha visto la proiezione della famosa pellicola Nemico Pubblico che tratta proprio del rapporto tra informazione, controllo da parte delle istituzioni e libertà di espressione. La serata è proseguita con il documentario Freedom Downtime, sulle vicende di Kevin Mitnick e dei movimenti politici e di protesta sorti a seguito del suo arresto e durante il periodo della sua detenzione.

Un sistema operativo online

Mentre i colossi dell'informatica si sfidano a colpi di innovazione con i loro sistemi operativi c'è chi ha deciso di tentare un approccio diverso alla gestione dei dati del PC. iCloud è il primo sistema operativo gratuito online. Non si tratta solo di un'interfaccia per gestire da remoto i nostri documenti o i programmi, ma di un vero e proprio PC su Internet dotato di software, hard disk virtuale per i nostri dati, e piena connettività con Internet: basta aprire il browser, collegarsi all'indirizzo http://icloud.com, inserire i propri dati ed accedere al PC sul Web. L'interfaccia è molto simile a quella di Windows Vista, e dispone di oltre 30 programmi che vanno da quello di videoscrittura alla gestione immagini, fino ai videogames. L'unico limite di iCloud è la compatibilità con il solo Internet Explorer 7. A breve i programmatori dovrebbero correggere questo "difetto".

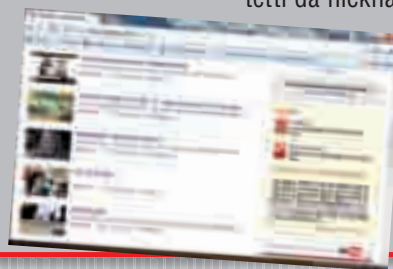
CHIUDE ANIMEDB... ADDIO ALLO STREAMING?

Era il più importante portale per lo streaming video, ma come spesso accade per le cose belle è stato chiuso, questa volta per sempre. Parliamo di AnimeDB, un vero e proprio sito di culto per gli appassionati di film e telefilm: questo portale, dopo una piccola registrazione, forniva i link a ogni genere di contenuto multimediale, compresi i telefilm americani aggiornati alla programmazione USA, i film appena usciti nelle sale e tonnellate di cartoni animati. AnimeDB dalla nascita aveva collezionato migliaia di utenti, costringendo gli amministratori a migrare su servizi sempre più costosi per accogliere un crescente numero di iscritti. Purtroppo nel nostro Paese anche la sola segnalazione di link a contenuti protetti è punibile dalla legge, per cui dopo anni di resistenza anche AnimeDB si è arreso. Si tratta di una perdita importante ma che non ha fermato il fenomeno dello streaming sul Web: sono decine i siti simili a AnimeDB che spuntano ogni giorno, per non parlare dei P2P dai quali è possibile scaricare praticamente di tutto liberamente.

UN IPOD SHUFFLE? 15 EURO

Premesso... non lo troverete mai a questo prezzo. Però 15 euro sono l'effettivo costo dei materiali necessari per costruire un nuovo iPod Shuffle. A togliersi lo sfizio di vedere cosa nascondeva la scocca del nuovo lettore multimediale di Apple sono stati i redattori della rivista iSuppli che hanno impiegato pochi minuti per disassemblare il loro iPod Shuffle ed estrarre ogni componente. Tra i pezzi più costosi che costituiscono il lettore c'è chiaramente il piccolo disco da 4 GB e il processore: solo questi due componenti costano 10 euro. I restanti 5 sono ripartiti tra batteria, condensatori, scocca, presa per le cuffie e altro. Considerando che lo Shuffle viene venduto a circa 80 euro, possiamo capire quanto Apple guadagna per ogni lettore venduto: certo, vanno sottratte le spese di progettazione, la distribuzione, e altre spese vive, ma il guadagno netto dovrebbe aggirarsi comunque su circa 40 euro... la metà. Mica male Apple.

YOU TUBE, IN COREA, INVITA ALLA DISERZIONE

Abbiamo parlato spesso di come i colossi del Web pieghino la testa di fronte ai regimi totalitari dell'estremo oriente, pur di vendere il loro prodotto. Questa volta invece segnaliamo il comportamento virtuoso di YouTube, che si è esposta alle critiche del governo Coreano, per aver dirottato i suoi utenti su portali di altri Paesi. Ma andiamo con ordine: dal primo aprile la Corea ha approvato una legge che obbliga i provider con più di 100.000 utenti a registrare gli accessi di ogni navigatore e individuarlo richiedendo, oltre al nome e cognome, anche codice fiscale e indirizzo. In questo modo il governo ha la possibilità di monitorare la sua attività e intervenire in caso di reati legati alla pubblicazione di video "sconvenienti" per la censura. Anche YouTube ha dovuto sottostare alla legge, ma ha trovato un modo per non perdere i suoi utenti reindirizzandoli dal portale coreano a quello inglese, fuori dalla giurisdizione del governo di Pyongyang. Così gli utenti coreani hanno ancora la possibilità di postare ogni tipo di contenuto protetti da nickname. Il gesto non è poi così eroico: la nuova legge aveva fatto crollare il numero di accessi al portale coreano, con un conseguente danno economico. Viva la libertà, pardon, i soldi!

HOT NEWS

HACKER CINESI SPIAVANO OLTRE 100 PAESI

Sembra la trama di un film di James Bond: dei ricercatori canadesi hanno scoperto una "ghostnet" (una rete fantasma) con cui hacker cinesi monitoravano l'attività di oltre 1300 computer delle principali organizzazioni mondiali.

Erano riusciti a bucare i firewall di CIA, FBI e governi di vari Paesi per collegarsi direttamente a PC con informazioni Top Secret. in più, con sistemi di remote control, azionavano le webcam collegate ai PC per vedere e ascoltare conversazioni riservate. I governi di mezzo mondo hanno chiesto alla Cina spiegazioni per questo gesto "ostile", ma pare che a Pechino nessuno ne sapesse nulla: ufficialmente la Cina è contro la pirateria e lotta perché che casi come questo non si verifichino.

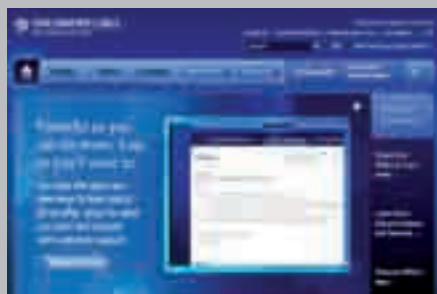
ARRIVA L'IPHONE NANO... MA È CINESE

Si chiama M188 ed è prodotto dall'azienda cinese CECT, ma tutti ormai lo hanno ribattezzato iPhone Nano. In attesa che Apple produca un modello in miniatura del suo smartphone, ecco il modello tarocco. Sembra davvero una versione mignon dell'iPhone: stesso look, stessa interfaccia a icone, stessa collocazione dei pulsanti. Ma la dotazione del telefonino di CECT è molto diversa da quella originale: non ha le connessioni UMTS e Wi-Fi, ma integra una radio FM e un alloggiamento Dual Sim. Se non volete attendere l'uscita di un iPhone Nano "vero", allora potete acquistare il CECT su eBay a circa 100 euro. Armatevi di soldi e pazienza però: per far arrivare il piccolo smartphone dalla Cina servono almeno 15 giorni e le spese di spedizione costano quasi quanto il telefonino.

GAMESTOP NON CI SIAMO!

È il Mac Donald's dei videogiochi, con punti vendita in tutto il mondo: parliamo di GameStop, catena di negozi di intrattenimento digitale, videogiochi, console e accessori. Recentemente il colosso della vendita di giochi è stato accusato di pratiche poco corrette nei confronti dei suoi clienti. Non tutti sanno infatti che esiste una clausola del contratto dei dipendenti di GameStop che li autorizza a prelevare un gioco appena uscito e provarlo gratuitamente per 4 giorni prima di restituirlo al negozio. Fin qui nessun problema: è utile per GameStop che i suoi commessi conoscano bene il prodotti che vendono, se non fosse per il fatto che i giochi usati vengano poi rimpacchettati e venduti come nuovi.

TARIFFE GONFIATE PER FILM E SOFTWARE

Vuoi scaricare film copiati, software e altro? Bene, allora dovrai pagare di più per la tua connessione. Questo è il senso dei nuovi abbonamenti proposti dal provider Time Warner Cable (la stessa Warner dei film) che ha stabilito un limite di Gigabyte alla sua connessione flat. L'abbonamento base, dal costo di

circa 25 dollari, prevede una capacità di download fino a 40 GB, oltre i quali gli utenti pagheranno 1 dollaro per ogni GB aggiuntivo. Certo, c'è la possibilità di eliminare la soglia, ma in questo caso si dovranno sborsare circa 60 dollari al mese, una cifra un po' esosa per una connessione a Internet. Le associazioni dei consumatori americani non hanno perso tempo, denunciando Time Warner, che però si è difesa sostenendo che le tariffe sono ancora sperimentali e che in molti casi saranno addirittura più vantaggiose delle precedenti, visto che sono più economiche per chi usa Internet solo per navigare e guardare la posta. Vedremo...

Il mondo visto con gli occhi dell'hacker

SAI PERCHÈ

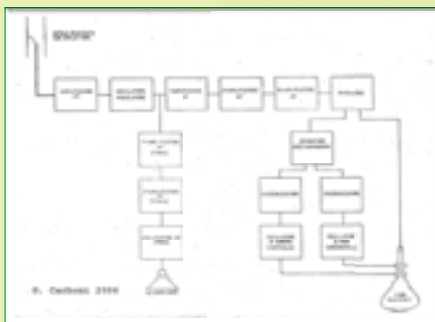
Le cose funzionano. Non ci si chiede mai il perché: compriamo una cosa e la usiamo così com'è, fidandoci di chi l'ha fabbricata. Quando non funziona bene, la portiamo a riparare; quando smette di funzionare, ce ne liberiamo per comprarne una nuova. Nessuna morale anticonsumistica: è lo stile di vita di oggi e a questo ormai ci siamo adeguati quasi tutti. Ma un hacker vede le cose in maniera differente. Hacker, innanzitutto, non vuol dire solo "smanettone", persona che vive perennemente collegata a Internet e con le mani sulla tastiera del PC. Un hacker è una persona curiosa di natura, che vuole capire come e perché le cose funzionano fino ad adattarle e personalizzarle secondo le proprie esigenze.

:: Il computer

È vero, per noi tutto inizia dal computer. È il primo oggetto di cui studiamo a fondo struttura e funzionamento tanto da trasformare il PC in un'estensione della nostra mente e delle nostre mani. La cosa importante, però, è che questa conoscenza, costruita pazientemente nel corso del tempo, arrivi al punto di modificare il nostro approccio alla vita e agli oggetti di uso quotidiano.

Un computer così l'abbiamo visto chissà quante volte, ma ci siamo mai chiesti il perché del suo funzionamento?

Ciò che ci interessa non è tanto che la scheda madre ospiti il processore, la memoria e così via ma che l'alimentatore del computer offrà una tensione stabilizzata di 12V, una duale di + e -5V e un notevole amperaggio, e di conseguenza che con un vecchio alimentatore da PC recuperato potremmo, per esempio, alimentare un lettore CD. In più un computer recuperato, anche un vecchio 386, dispone di porte seriali e parallele con cui possiamo pilotare i più disparati aggeggi elettrici ed elettronici, sviluppando eventualmente del software ad hoc. Alcune idee? Costruiamo un case simile a quello dei videogame Arcade, quelli che troviamo al bar e in sala giochi per intenderci, e adattiamo al suo interno un vecchio PC con tanto di monitor per farci girare MAME e la nostra collezione di ROM d'epoca. O perché invece non fare a meno del monitor e creare un componente in formato rack da associare all'impianto stereo per ascoltare la collezione di MP3 anche in vacanza? Con Linux, un ricevitore a infrarossi con relativo

Un videogioco da bar? Potrebbe, ma potrebbe anche essere il nostro vecchio PC adattato appositamente per MAME!

Lo schema a blocchi di un dispositivo ci aiuta a capire la funzione di ogni suo singolo componente.

telecomando e un po' di manualità non è una cosa complicata.

:: I "mattoni" degli oggetti

Ogni cosa, che sia un computer o un elettrodomestico, difficilmente è costituita da un unico componente. Nella maggior parte dei casi, diversi elementi interconnessi collaborano per permettere il funzionamento del dispositivo, e ognuno di essi ha una propria funzione autonoma. Aprendo e studiando un vecchio elettrodomestico, potremmo facilmente creare uno schema a blocchi del suo funzionamento, identificare i singoli componenti e, per ciascuno, definirne la funzione principale. Già questa nuova ottica ci apre la porta per un mondo interessantissimo, ma un hacker non si accontenta mai e la fame di conoscenza è immensa: proviamo a spingerci oltre.

:: Le misure dei mattoni

Ora sappiamo perfettamente come è composto un dispositivo e a cosa servono nel suo schema a blocchi i singoli elementi di cui è formato. È quindi arrivato il momento di spingerci un po' oltre e di prendere in esame ogni singolo componente. Il suo scopo l'abbiamo capito, ma non ci interessa più sapere a quale proposito è stato costruito, ciò che stuzzica di più la nostra curiosità è che cosa effettivamente può fare. Smontiamo un vecchio televisore a tubo catodico: otterremo per esempio una pulsantiera. Originariamente è stata creata per comandare le funzioni principali del televisore, ma la sua natura è semplicemente l'essere composta da diversi pulsanti, a prescindere dai comandi che questi impartivano nel dispositivo originale. Smontata e individuati i punti di ingresso e di uscita dei segnali, potremo riutilizzarla in qualsiasi altro nostro progetto che necessiti di pulsanti per l'attivazione di determinate funzioni. Dallo stesso televisore otteniamo anche una sezione di amplificazione audio dalle caratteristiche notevoli: possiamo recuperare altoparlanti e amplificatore di potenza, di solito montato su una scheda separata. Questo genere di amplificatore di solito ha bassi potenti e sonorità morbide, non sarà da alta fedeltà ma sarebbe ottimo per il lettore MP3 (magari auto-

Altoparlanti per televisori, hanno una buona potenza e in un mobile adeguato anche la resa acustica non è da disprezzare.

costruito da un vecchio PC). Non ci serve altro che identificare la tensione di alimentazione di cui necessita per recuperare o costruire un alimentatore adeguato e montare tutto dentro un mobile appositamente realizzato.

:: L'importanza della curiosità

Hacker significa anche soprattutto questo. Non limitiamoci mai all'apparenza delle cose, ma scaviamo in profondità. Trasformiamoci in vere e proprie spugne e assorbiamo ogni informazione, ogni minima nozione che troviamo intorno a noi. Manteniamo viva la nostra curiosità, soprattutto nei campi che ci appassionano di più, e solo allora potremo definirci veri hacker.

Il portatile è stato rubato? Se c'è installato Boinc trovarlo è molto semplice

BOINC! COMPUTER RITROVATO

Stando all'FBI, ogni anno, nei soli Stati Uniti, vengono rubati due milioni di notebook. Anche fermandosi a questa cifra, e senza tenere conto di altri formati (netbook, fissi, eccetera), possiamo ben dire che anche noi corriamo il rischio di vederci sparire sotto il naso il nostro amato elaboratore. Che fare? Oltre alle protezioni "attive", che prevengono il furto, è il caso di pensare anche a mezzi che ci consentano di recuperare il computer se questo, alla fine, viene rubato. Tra le migliori c'è BOINC, un software che serve a tutt'altro, ma che all'occorrenza si utilizza pure come "rilevatore" di dove si trova il computer in un dato momento. Ma andiamo con ordine presentando innanzitutto il protagonista di queste pagine.

:: Mi chiamo Boinc

Boinc (Berkeley Open Infrastructure for Network Computing) è un progetto, portato avanti dall'università di Berkeley, che consente di sfruttare "l'idle time", cioè il tempo d'inattività dei computer, per convogliare la potenza di calcolo sprecata in opere benefiche. Così, per esempio, se lasciamo il computer inattivo, Boinc lo sfrutta per eseguire i calcoli necessari alla ricerca scientifica. Ovviamente i benefici di un progetto simile vanno considerati su vasta scala, pensando a tutti i computer che vi aderiscono. Tutti insieme, infatti, formano una rete dalla mostruosa potenza di calcolo. Boinc non

è certo il primo esempio di "grid computing", ma è uno dei migliori e più sicuri progetti non commerciali di questo tipo. E la sua lunga tradizione non fa che confermare la buona impressione: pensiamo, infatti, che Boinc sta alla base, fin dalla prima versione, del progetto SETI@home, dedicato all'analisi dei segnali extraterrestri ai fini della ricerca di altre forme di vita nello spazio.

SETI@home è stato uno dei primi esempi di "grid computing", nonché il debutto ufficiale della tecnologia BOINC.

:: Come funziona

Il funzionamento di Boinc si basa su un software da installare in ogni computer che aderisce al progetto. Il software è, a tutti gli effetti, un client che sfrutta l'idle time delle CPU e di alcune GPU (quelle Nvidia che supportano CUDA), e che è gestito e coordinato a seconda delle necessità dai server della Berkeley University.

Va da sé che l'architettura client-server è quella che torna utile per il nostro scopo: recuperare un computer rubato. Prima di entrare nei dettagli della questione, comunque, vediamo di aderire al progetto Boinc. Per farlo, andiamo sul sito boinc.berkeley.edu/download.php, clicchiamo su Download BOINC (disponibile in versione Windows), e quindi scarichiamo e installiamo il software. Facciamo doppio clic sul file, quindi (se usiamo Windows Vista) clicchiamo su Esegui e poi su Consenti. Si avvia la procedura d'installazione: clicchiamo su Next, spuntiamo la casella I accept the terms in the license agreement, clicchiamo su Next, ancora su Next, su Install e, al termine dell'installazione, su Finish.

Ora non resta che riavviare il computer, cliccando su Yes nel box visualizzato. Una volta riavviato il computer, compare la procedura di connessione di Boinc. Sostanzialmente, si tratta di scegliere un progetto al quale dedicare le risorse del proprio sistema. Clicchiamo su Avanti, poi sul progetto desiderato (se non sappiamo di cosa si tratta consultiamo l'elenco su boinc.berkeley.edu/projects.php), ancora su Avanti. A questo punto in "Informazioni utente" riportiamo i dati richiesti, per iscriverci. Una volta inseriti, clicchiamo su Avanti e, dalla finestra Sei connesso al progetto clicchiamo su Fine. In genere, a questo punto si apre una finestra del nostro browser, coi dati dell'account presso il progetto scelto. Al momento, possiamo chiuderla.

Il progetto Rosetta fa bene alla scienza e... a chi è stato derubato del proprio computer. Provare per credere.

:: Via alla caccia

Una volta che la tecnologia Boinc è stata attivata nel computer, eccoci alla parte più sfiziosa: sfruttarla per individuare dove si trova un computer. In genere, chi ruba un computer accende il dispositivo almeno una volta. E molto probabilmente lo lascia inattivo per un tempo sufficiente a far entrare in azione Boinc (ovviamente si deve essere collegati a Internet). Bastano anche pochi secondi, a questo punto, per far scattare la trappola. Per rintracciare il computer, infatti, colleghiamoci al sito relativo al progetto al quale abbiamo aderito. Per esempio, nel caso di Rosetta (dedicato alla ricerca medico-scientifica), boinc.bakerlab.org. Da qui, clicchiamo su login/out (è una voce piccola, che compare in alto a destra). Inseriamo i dati di autenticazione scelti poco fa, ed eccoci nel nostro account. Da qui, cerchiamo la voce Last contact. Clicchiamoci sopra, poi clicchiamo sul computer che stiamo cercando e, quindi, su Show IP Address.

Il servizio ci presenta, oltre ad una serie di indicazioni tecniche, anche la mappa del nodo di connessione

Quello che compare è, a tutti gli effetti, l'indirizzo IP relativo alla connessione utilizzata da chi ha rubato l'elaboratore. Il che equivale a un indizio di grande valore, che possiamo sfruttare in vari modi. Per esempio, effettuando un Whois. Per farlo, ci basta andare su un servizio web apposito, come http://www.ip-adress.com/ip_tracer/, riportare nella casella l'indirizzo IP e cliccare su Track IP,host or website.

Le informazioni ottenute possono darci un'idea della posizione in cui si trova il nostro computer rubato, o comunque saranno sufficienti per contattare le Autorità e fornire precise indicazioni sull'ultimo luogo dove si è connesso.

Ericsson ha presentato un portatile con integrati un GPS e un sistema capace di bloccare il PC da remoto. Sarà difficile da rubare ma anche tutelare la privacy

NOTEBOOK RINTRACCIABILI

Arriviamo al bar, come tutte le mattine. Posiamo la borsa accanto a noi e ci beviamo un buon caffè. Allunghiamo la mano per riprenderla, e annaspiamo nel vuoto. Certo, l'abbiamo posata per pochi secondi, era proprio vicino a noi, non abbiamo notato nessuno… Eppure la borsa e il portatile che conteneva sono svaniti nel nulla e non possiamo fare altro che andare a sporgere una denuncia. Ogni anno, in Italia, migliaia di computer portatili spariscono nei modi più vari: dai furti di portatili chiusi in macchina, con contorno di vetri sfondati, fino alle sottrazioni con destrezza nei bar, nei ristoranti, sui treni. Sottrazioni che vengono fatte anche a meeting aziendali, riunioni, nelle sale d'attesa o anche direttamente in ufficio o in casa. Il problema è talmente sentito che i prodotti per tutelarci si sprecano: lucchetti con cui legare i portatili alla scrivania, sensori di movimento che scattano quando il portatile si muove senza di noi, software dedicato alla rintracciabilità e molto altro.

Ericsson ha presentato un PC protetto dai furti con GPS integrato e chip dedicato. Peccato che i risvolti sulla privacy siano preoccupanti.

::Soluzioni software

La comunità Open Source ha da tempo cercato di rimediare al problema con la creazione di Adeona: un software che si installa sul portatile e che tiene traccia di ogni suo movimento, informandone un server di controllo. I pacchetti di dati inviati includono, se disponibile, la posizione GPS e l'indirizzo IP, allo scopo di risalire almeno alla zona in cui il portatile risulta attivo. Adeona si può scaricare dal sito adeona.cs.washington.edu. In commercio esistono altre soluzioni, generalmente simili, che permettono di avere lo stesso grado di protezione. Ci sono persino sistemi fai da te, come abbiamo visto nelle pagine precedenti. Il problema, semmai, è

Kensington è specializzata nella creazione di sistemi antifurto per notebook. Attualmente, un buon lucchetto è ancora la soluzione migliore.

che queste soluzioni sono esclusivamente software: basta una riformattazione della macchina per ottenere un computer pulito. Nella realtà, tutti i produttori di notebook hanno database interni di computer rubati, che ne riportano i numeri di serie. Nel caso in cui un incauto acquirente di merce rubata portasse il suo computer "nuovo" in riparazione, questi database permetterebbero di rintracciare il proprietario legittimo e provvedere alla restituzione del maltolto. Per questo motivo, in caso di furto, è sempre bene comunicare l'avvenimento al produttore, allegando una copia del verbale di denuncia. Nella maggior parte dei casi, purtroppo, dovremo subire passivamente il furto: il 90% dei computer rubati non viene mai più recuperato.

:: L'hardware aiuta

Per questo, l'annuncio di Ericsson della commercializzazione del suo notebook F3607gw viene vista come un sistema definitivo contro i ladri. Il computer incorpora un sistema GPS, non sganciabile, capace di monitorarne in continuazione la posizione. Al suo interno è contenuto anche un circuito, compatibile con la Anti-Theft Technology di Intel, capace di bloccare completamente il computer su richiesta del proprietario, salvo poi sbloccarlo quando viene recuperato. Dal punto di vista della sicurezza si tratta certamente di un grande passo avanti ma, contemporaneamente, di un pericolo in più. Il passo avanti è dovuto al fatto che il furto di un notebook del genere risulta sostanzialmente inutile: basta un collegamento a Internet, anche dopo una riformattazione, per bloccare la macchina. D'altra parte, la possibilità di usare un computer che può essere tracciato a nostra insaputa crea problemi di ampia portata, anche se i produttori promettono che questa tecnologia garantisce la privacy.

GIÚ LE MANI

Ecco alcuni suggerimenti su come evitare che una gita con il nostro portatile si trasformi in un viaggio dai carabinieri per denunciarne il furto o per segnalare la sottrazione dei dati che contiene.

- Non lasciare mai il portatile incustodito, specialmente in stanze che non sono chiuse a chiave.
- Ancora il notebook alla scrivania durante i meeting, le riunioni, gli incontri di lavoro che prevedono pause anche brevi.
- Riponi il notebook nella sua borsa quando non lo utilizzi.
- Controlla sempre la borsa nei bar o nei ristoranti, magari incastrando la tracolla tra le gambe.
- Nei viaggi in auto, aggancia sempre il portatile a qualche parte fissa. Se riposto, colloca la borsa in modo che non sia visibile e che non permetta ad alcuno di impossessarsene rompendo il vetro, magari ad un semaforo.
- In hotel, affida sempre il PC al personale della reception.
- Non prestare mai il notebook.
- Mantieni sempre una copia di sicurezza dei dati sul notebook, magari usando un servizio online.
- Utilizza tutti i sistemi di cifratura disponibili: quelli inseriti nel SO vanno bene, altrimenti usa prodotti Open Source o commerciali.

Undercover, www.orbicule.com/undercover, è il software antifurto per Mac. Funziona bene ma non offre garanzie contro i ladri più smaliziati.

Ogni computer, infatti, è identificato univocamente, in barba alle polemiche di qualche anno fa alla attribuzione di numeri di serie alle CPU.

:: Addio privacy

Questa identificazione, già da sola, permetterebbe di imporre agli utenti aggiornamenti obbligatori, correlare abitudini di navigazione agli utenti in modo univoco e molte altre pratiche che possono essere utili da un lato ma devastanti per la privacy dall'altro. L'unione di questi meccanismi con ricevitori GPS integrati rende la prospettiva ancora più devastante, permettendo persino la geo localizzazione degli utenti. Il tutto senza considerare che il chip hardware che può disattivare il notebook è in grado di interagire con il software e, per questo, può essere almeno teoricamente soggetto ad attacchi. Per essere più espliciti, non è remota l'ipotesi che qualcuno possa trovare il modo di carpire i segreti di questo chip, magari rubandoli al server di gestione del sistema, per bloccare ignari utenti e ricattarli per fargli riprendere il controllo del loro hardware. Alla luce di poche considerazioni, la prospettiva di sicurezza vista inizialmente viene completamente ribaltata e l'arrivo di questi sistemi di sicurezza non sembra più così tanto piacevole come poteva apparire in origine.

TUTTO IL SOFTWARE CHE VUOI

Non sono una novità ma si stanno diffondendo sempre di più: i programmi "condivisi"

Quando il computer diventa il nostro hobby principale, inizia a farsi sentire la terribile fame di software. Programmi di tutti i tipi, dai più semplici ai più complessi, dai più seri ai più divertenti. Per un hacker la fonte principale di software è la comunità Open Source, a volte perché è indispensabile poter disporre del codice sorgente, a volte invece perché si vuole essere "alternativi" a tutti i costi. In effetti, moltissimi programmi tra i più usati sono Open Source: da OpenOffice.org a The Gimp, da Firefox e Thunderbird allo stesso Linux. Non sempre però questo è sufficiente per placare la nostra fame, e allora si va ad attingere al pozzo del peer to peer. Quali che siano le motivazioni, scagli la prima pietra chi non ha mai scaricato un software commerciale con eMule, magari con tanto di crack o keygen per poterlo sproteggere. Crediamo sia inutile ricordare che farlo è illegale e non esistono scuse quali "volevo solo provarlo" oppure "era un'urgenza, l'avrei comprato". Tuttavia il dato di fatto è che prelevare un programma via P2P è prassi più frequente di quello che non si ammetta. Vi abbiamo avvisati, a voi usare con giudizio le informazioni che si trovano in queste pagine.

:: La ricerca della vena

Come un buon minatore sa riconoscere i segnali che indicano la possibile presenza di una vena d'oro nella miniera che sta scavando, allo stesso modo si devono leggere adeguatamente i risultati delle

Una ricerca su eMule. Data la popolarità del programma, i risultati sono moltissimi, ma probabilmente quelli falsi sono numerosi.

ricerche con il Mulo, perché in realtà trovare esattamente quello che si sta cercando non è poi così semplice. I motivi sono diversi, ma è sufficiente avere ben presente che non sempre il file che stiamo scaricando corrisponde a quello che il suo nome dice e che non sempre si tratta di un prodotto realmente utilizzabile.
La regola fondamentale è: più un programma è famoso e usato, più è facile l'inquinamento dei risultati di una ricerca per poterlo scaricare. Per inquinamento dei risultati intendiamo che la possibilità che un file sia fasullo è direttamente proporzionale alla diffusione del programma che stiamo cercando. Ce ne possiamo rendere conto facilmente inserendo nella casella il nome di un programma molto conosciuto, per esempio Photoshop o Office. Otterremo sicuramente centinaia o migliaia di risultati (sempre che il nostro mulo sia configurato a dovere), tra cui dovremo scegliere quello che effettivamente è il più adatto a essere scaricato. Ma come possiamo fare?

Crack e generatori di seriali spesso nascondono virus e trojan, ma frequenti sono anche i falsi allarmi degli antivirus. Stiamo comunque attenti.

:: L'oro dei folli

Pirite, niente altro che pirite. È un minerale metallico, dalla colorazione molto simile a quella dell'oro, ma dal valore pressoché nullo rispetto al metallo prezioso. Viene chiamata così perché solo i folli la possono scambiare per oro vero. Anche per il software via peer to peer vale la stessa cosa: i file fasulli sono moltissimi e si va dal solito pornazzo a cui è stato semplicemente cambiato il nome al file completamente vuoto (nel vero senso della parola), creato appositamente per prendere per il naso (o un'espressione simile) gli scaricatori. eMule ci dà qualche strumento per poterci mettere al riparo da simili eventualità, ma purtroppo per poterli usare bisogna iniziare a scaricare il file in questione. La prima cosa, ovviamente, è tenere d'occhio le proprietà del file. Facendo clic destro sul presunto programma e scegliendo Informazioni sul File, possiamo controllare che la scheda Generale della finestra mostrata riporti il tipo di file come verificato. Se stiamo scaricando un RAR e questa finestra ci comunica che in realtà il file è un AVI, possiamo anche interrompere il download perché sarà il solito film porno.

La finestra delle informazioni sul file in download. Se si tratta di un fake ce ne possiamo accorgere già da qui.

L'altro strumento fondamentale è l'anteprima. Se abbiamo scaricato una buona percentuale del file e la finestra delle informazioni ci conferma che sia un archivio compresso o una ISO, possiamo creare un'anteprima che verrà aperta con il programma corrispondente e potremo così verificarne direttamente il contenuto. Un'ultima cosa per quanto riguarda i file: ormai con la banda larga non ci si pone più il problema delle dimensioni, ma a volte pare che qualcuno si faccia ancora delle remore e, quando crea la copia del programma, ne distribuisca una versione "stripped". Si dicono tali i software da cui sono stati eliminati elementi aggiuntivi non indispensabili per il loro funzionamento ma comunque presenti sui supporti originali: grafiche e clip art per programmi di grafica, sequenze animate per i giochi e così via. Se non ci interessano, va bene così; tuttavia sicuramente spulciando bene troveremo anche versioni più complete degli stessi programmi.

:: Controindicazioni

Inutile dire che scaricare un programma da una fonte come il peer to peer non è mai una buona idea: a meno che il nostro computer non sia un fortino inespugnabile, la possibilità di beccarsi un virus o un trojan è tutt'altro che remota. E spesso non è il programma a portarselo dietro, ma il crack o keygen che lo accompagna. Sempre più spesso Avast e altri antivirus riportano come trojan generici qualunque tipo di crack, patch, keygen e simili per scoraggiare dal loro utilizzo, anche se la minaccia non è sempre reale. Sta a noi usare un po' di buon senso.

NUOVA VITA AL TUO PORTATILE

Cinque cose che si possono fare per recuperare il vecchio notebook

I notebook soffrono di obsolescenza precoce, dovuta al fatto che il software diventa sempre più pesante e le limitate possibilità di aggiornamento dell'hardware ci costringono a cambiarlo dopo pochi anni di servizio. Quando arriviamo al punto di non poter più fare a meno di comprare un nuovo notebook, ci si pone il dubbio di cosa fare di quello vecchio. Possiamo rivenderlo, naturalmente, ma ciò che ne ricaveremmo sarebbe ben poca cosa rispetto al prezzo del nuovo. Oppure possiamo mettere in moto l'ingegno e recuperarlo in qualche modo: ecco qualche consiglio.

:: L'aggiornamento

Un notebook usato, di marca, per diversi mesi può vedere allungata la propria vita operativa con l'aggiornamento dell'hardware. In generale possiamo acquistare nuova RAM, un disco più capiente e in certi casi anche un processore più recente, e già questo aiuterebbe a reggere il carico di lavoro ancora per un po' di tempo. Tuttavia anche in questo modo ci troveremmo prima o poi con lo stesso problema. Perché allora non spingiamo oltre le possibilità hardware del nostro piccolo aggiungendo funzionalità non previste in origine? Per esempio, possiamo armarci di saldatore (e della conoscenza necessaria, naturalmente) per aggiungere moduli Bluetooth, GPS e magari 3G a un notebook che ne è sprovvisto e poterlo così usare per collegarci a Internet anche quando siamo in vacanza, dove non sempre è disponibile una linea adeguata, o per sfruttarlo come navigatore per programmare il nostro viaggio. Si tratta in effetti di moduli USB ormai non più grandi di un'unghia: con un po' di pazienza possiamo trovare uno spazio

all'interno del case del notebook per installare la circuiteria interna di un hub USB alla quale collegare le elettroniche dei dispositivi aggiuntivi.

:: Picture Frame

Apriamo il nostro notebook e osserviamolo bene. Istintivamente, la vista si sofferma innanzitutto sul display, luminoso e dalla risoluzione più che accettabile. Se siamo in grado di visualizzare le foto scattate con la fotocamera, perché non recuperare tutto il blocco per creare una cornice digitale come quelle che si trovano oggi in commercio? In effetti, si tratta di smontare il tutto e riorganizzarlo per poterlo inserire in un nuovo case, magari a forma di cornice da appendere al muro. Per il suo utilizzo ci basta lasciare accessibili le porte USB, a cui collegare chiavette di memoria con nuove foto e filmati, ed eventualmente mouse e tastiera wireless per la manutenzione periodica. Chi vuole può spingersi anche oltre, adattando una pellicola sensibile al tocco al display della nuova cornice e programmando un'interfaccia utente per pilotare lo slide show delle nostre foto.

Porte USB aggiuntive, con tanto di memoria flash, per un netbook: http://www.ultramobilegeek.com/2007/08/adding-internal-usb-and-internal.html.

:: Media Center

È un po' l'estensione naturale della Picture Frame: possiamo anche creare un lettore multimediale dal grande schermo e adattarlo per l'uso negli ambiti più disparati. Per esempio, sistemando l'elettronica in un case slim come quello dei lettori DVD possiamo usarlo accanto al televisore integrandolo nell'impanto home theatre, così potremo guardare su grande schemo anche i film scaricati da Internet, oppure sostituire il display con uno più piccolo e panoramico (un 7 pollici è economico e facilmente recuperabile) per farlo diventare il Car PC multimediale dei nostri sogni. La cosa fondamentale in questo caso è trovare un'interfaccia di controllo piacevole e facile da usare. Windows Media Center può andare bene se lo abbiamo già, ma possiamo anche optare per software gratuito installando Linux, per cui esistono già diversi progetti per l'implementazione di un Media Center basato sul pinguino (GeeXBoX è un perfetto esempio, lo troviamo all'indirizzo http://geexbox.org/en/index.html).

GeeXBoX è perfetto per creare un Media Center casalingo partendo da un vecchio notebook che ormai non usiamo più.

:: Home Server

Quando si guasta il display del nostro notebook, difficilmente pensiamo alla riparazione: i costi di questo componente non giustificano lo sforzo, soprattutto confrontandoli con il prezzo di un nuovo portatile. Senza alternative, quindi, un notebook con il display rotto (e non si parla della retroilluminazione, che è più facile da riparare) finirebbe quasi certamente in discarica. Lo stesso spesso succede quando a guastarsi è la tastiera, benché più economica come pezzo di ricambio. Possiamo usarlo per un po' con un monitor o una tastiera esterni, ma a questo punto verrebbe meno la praticità propria del notebook. Perché allora non trasformarlo in un server casalingo, per cui non necessitiamo del display e della tastiera? Possiamo collegarci da remoto usando VPN o altri sistemi, il monitor esterno lo usiamo solo per l'installazione del sistema operativo, ovviamente Linux, poi possiamo anche farne a meno. Avremo un computer che consuma poco che fa da file server e da server di stampa, ma possiamo anche configurarlo come server Web per creare i nostri siti in locale.

:: Upgrade estetico

Ci ricolleghiamo un po' alla prima delle idee presentate e torniamo a parlare di aggiornamento. A volte, infatti, abbiamo spremuto veramente il massimo dal nostro notebook e non è possibile farci entrare nemmeno uno spillo da quanto l'abbiamo imbottito di moduli extra. Ma siamo hacker, non caporali, quindi ci spingiamo oltre e mettiamo in cantiere un upgrade estetico per il case del nostro "Frankenbook". Ricostruiamo l'intero case in legno, magari ridimensionandolo per meglio accomodare quanto nel corso del tempo abbiamo aggiunto, o comunque in previsione di ulteriori upgrade hardware. Oppure possiamo semplicemente abbellirlo, dandolo in mano a un artista che con l'aerografo può trasformarlo in un'opera d'arte portatile e tecnologica. In effetti, tutto ciò che ci serve è la nostra fantasia e un po' di tempo da dedicare a quello che potrebbe diventare facilmente un nuovo hobby che può estendersi anche oltre il mod di un semplice notebook: Benjamin Heckendorn ne dà prova sul suo blog all'indirizzo http://benheck.com.

Il "Legnatile", un notebook il cui case è stato magistralmente ricostruito completamente in legno: su http://www.zaverio.org.

Un database a nudo

Le tecniche di SQL Injection permettono di ottenere il controllo completo di un DB partendo da qualsiasi campo ci venga richiesto di inserire

Quando si parla di SQL Injection si intendono tutte quelle tecniche adottate allo scopo di modificare il funzionamento di query a database agendo solo tramite le richieste di dati che un sistema fa all'utente. Storicamente, questo genere di attacchi si diffonde con i siti Web dinamici ma la sua presenza è di motlo anteriore: già con la nascita dei primi database, la SQL Injection era una tecnica già usata per capire il funzionamento di alcune applicazioni.

:: Un meccanismo fallace

I siti che chiedono di compilare campi di vario genere sono diffusissimi: si va dall'inserimento di un nome e una password per l'accesso ad aree riservate fino all'inserimento di vari dati, anche personali, per compiere una registrazione, inviare messaggi all'autore e via dicendo. Questi campi, codificati in HTML come tag INPUT, possono essere adattati nella loro rappresentazione a un tipo determinato di dati che ci aspetta ma sono stanzialmente liberi. L'HTML non ha specifiche di formattazione del testo in input ma solo, come è giusto, specifiche di rappresentazione. Così, la validazione è generalmente affidata ai Javascript che, tuttavia, possono risultare facilmente aggirabili. Per sua natura, a meno di sistemi di progettazione particolari, le pagine dinamiche accettano input indipendentemente dalla sua provenienza e questo consente di creare pagine di input ad hoc e di sottoporre input privi del controllo Javascript alla pagina che li dovrà elaborare. Di più: diversi utenti non

Qualsiasi modulo HTML può essere utile per un'azione di SQL Injection. I moduli preferiti, però, sono quelli di login.

hanno abilitato Javascript, il che presuppone che non avvenga alcun controllo sugli input immessi nelle caselle di testo. L'obbligare gli utenti ad attivare Javascript, viceversa, dà vita a problematiche di vario tipo, inclusi quelli di accessibilità. Con queste premesse, non è difficile trovare ancora oggi diversi siti completamente esposti a un attacco basato su SQL Injection. Il meccanismo è facile: non permettendo un controllo sui dati inseriti nei moduli e sapendo che la pagina che riceve i dati li utilizza in una query, inserendo linguaggio SQL in un campo di un modulo è possibile agire sul database in modi imprevisti dai programmatori. Ovviamente, le tecniche descritte richiedono un certo grado di analisi e una buona conoscenza, almeno in partenza, del linguaggio SQL. Negli esempi che seguono useremo Microsoft SQL server ma un buon attaccante cercherà di ottenere informazioni specifiche sul database usato, così da scegliere i suoi metodi di attacco in modo mirato.

:: Un esempio

Prendiamo, per esempio, una query di ricerca SQL banale: SELECT id FROM utenti WHERE nome = 'camporicevuto' and ingresso=true. Ad inviare i dati alla pagina che fa uso di questa query sarà un'altra pagina che farà corrispondere campo ricevuto al testo inserito dall'utente. Se questo utente inserirà il nome, come atteso, la query verrà eseguita correttamente. Pensiamo, però, a un utente che inserisca la stringa x' or 'a'='a --. La query risultante sarà questa: SELECT id FROM utenti WHERE nome='x' or 'a'='a' -- and ingresso=true. Grazie all'uso del costrutto or, corrisponderà a tutti i record della tabella utenti riportando come risultato gli id di tutta la tabella. La presenza dei due trattini, che in SQL contraddistinguono i commenti, il resto della query verrà ignorato, permettendo di superarla agevolmente. Nel caso di siti in cui è stato trascurato questo genere di attacchi, il risultato andrà dal consentire l'ingresso in un'area riservata al generare qualche errore su server.

Inutile tentare di entrare con la SQL Injection in siti creati con sistemi già pronti, specialmente se Open Source. I controlli da parte degli utenti minimizzano il problema.

Proprio gli errori possono essere la chiave di volta di attacchi ben più distruttivi. Pensiamo, per esempio, a un utente che inserisce nel campo un semplice apostrofo e dà l'invio. Il risultato, nella query precedente, sarà questo: SELECT id FROM utenti WHERE nome='''. In SQL, il triplo apice dà un errore che, se non indicato diversamente in fase di configurazione del server, dà vita a un evento http 500, seguito dalle specifiche utili per identificare e correggere il problema. In molti casi, quindi, l'attaccante può ottenere un risultato come il seguente:

Microsoft OLE DB Provider for ODBC Drivers error '80040e14'
[Microsoft][ODBC M icrosoft Access Driver] Syntax error in string in query expression 'nome='''.
/test.asp, line 52

::Danni e devastazioni

Proprio una segnalazione di errore nata per aiutare i programmatori a correggere un problema, però, fornisce indicazioni utili sulla struttura del database. In un sistema senza protezioni, questa sola indicazione può avere effetti devastanti perché bastano alcuni comandi per ottenere indicazioni vitali per un attacco in piena regola: nomi di campi coinvolti nelle query, nomi di tabelle, relazioni tra loro, indicazioni sugli indici e altro ancora. Per scoprire il nome della tabella e della prima colonna sotto attacco, per esempio, basta completare la query provocando un errore che ce li fornisca. In questo caso basta che il campo testo contenga ' having 0=0 --. La query risultante sarà SELECT id FROM utenti WHERE nome=' ' HAVING 0=0 -- and ingresso=true. In SQL, questo costrutto dà per forza errore perché è sbagliata la sintassi del costrutto HAVING e il risultato è l'ottenimento di un messaggio d'errore che segnala come utenti.nome non sia valido perché non aggregato tramite la clausola GROUP BY. Proseguendo con l'analisi, i risultati possono essere eclatanti: basta aggiungere questa clausola per il campo che il sistema stesso ci segnala per ottenere una mappatura completa della tabella interessata: SELECT id FROM utenti WHERE nome=' ' GROUP BY utenti.id HAVING 0=0 -- and ingresso=true. Aggiungendo man mano i campi indicati il nostro attaccante arriverà a non ricevere più errori. In questo caso, la struttura della tabella sarà quella indicata dopo la clausola GROUP BY. Inutile dire che con questa miriade di informazioni, chiunque abbia anche minime conoscenze di SQL Server può fare danni devastanti. Pensiamo, per esempio, alle conseguenze che si ottengono trasformando la query iniziale in questa: SELECT id FROM utenti WHERE nome=''; DROP TABLE utenti;--'. Basta un comando per veder distrutta la tabella,

Microsoft OLE DB Provider for ODBC Drivers error '80040e21'

ODBC driver does not support the requested properties.

/invio_pass_operatori.asp, line 29

Basta poco per riuscire ad ottenere un messaggio di errore che indichi all'attaccante il sistema di database usato. Da lì, condurre attacchi specifici è banale.

con gravissimi danni al sistema. Un'altra possibilità è quella di avvelenare il sistema con dati falsi, facendo inserimenti incontrollati: SELECT id FROM utenti WHERE nome=''; INSERT INTO utenti (nome) VALUES ('Provami');--'. In alternativa, l'attaccante può decidere di fare gli aggiornamenti che gli aggradano: SELECT id FROM utenti WHERE nome=''; UPDATE utenti SET nome='mionome';--'.

::Contromisure

Per ottenere un sistema protetto, quindi, è necessario che i programmatori facciano moltissima attenzione a validare correttamente qualsiasi input

Tutti i siti più diffusi dispongono di sistemi molto sofisticati per evitare le pratiche di SQI Injection. Volenti o nolenti anche gli altri siti si sono dovuti adeguare.

recuperato dalle pagine precedenti, specialmente se richiesto all'utente. La tecnica, in questi casi, è quella di ripulire gli input direttamente nella pagina di ricezione ma facendo molta attenzione: non dobbiamo rimuovere gli apici ma impedire i danni. Se il confronto avviene tra codici numerici, infatti, gli apici non servono e questo permette comunque di subire attacchi di SQL Injection. Allo stesso modo, gli apici compaiono in alcune scritte come elementi legittimi. Pensiamo, per esempio, a una persona che si chiama Marco D'Orta: l'apice è corretto e non vi sono tentativi di SQL injection in corso. Il trucco, quindi, può essere quello di impedire non tanto l'uso dei caratteri al di fuori di quelli canonici (cifre e lettere) ma di validarlo correttamente in base all'utilizzo nell'applicazione. Se ci aspettiamo un numero, per esempio, basta un semplice controllo per assicurarsi che l'utente non abbia inserito caratteri diversi da quelli consentiti. Un'altra contromisura indispensabile è quella di configurare il server Web per fornire messaggi di errore generici in sostituzione di quelli specifici oppure, soluzione caldamente consigliata, quella di intercettare gli errori nelle pagine e creare log visibili solo all'amministratore, mandando all'utente informazioni generiche. Un altro modo di tutelarsi è quello di pensare fuori dagli schemi durante la creazione delle query. Abitualmente, infatti, i programmatori tendono a realizzare query molto simili. Se il modulo richiede di inserire un nome e una password, infatti, il programmatore della pagina che riceve i dati tenderà ad usare il costrutto WHERE con una forma tipo: WHERE nome='' AND password=''. Questo costrutto permette a un attaccante di inserire Admin' – come nome, facendo ignorare al sistema la parte di autentica della password. Malgrado queste tecniche, però, basta fare attenzione per riuscire ad ottenere un sistema a prova di bomba. Certo, occorre una certa conoscenza del sistema su cui si vanno a considerare le autenticazioni ma è una conoscenza che deve essere obbligatoriamente alla portata di chi il sistema lo sta facendo.

INGRESSO LIBERO

Vediamo insieme i comandi più distruttivi che possono essere portati dall'attaccante durante le sue prove di SQL Injection. In questi esempi si pensa a un sistema di login che richiede un nome e una password.

Nome: ' having 0=0—
Password: qualsiasi
Risultato: L'eventuale messaggio di errore rivela il nome della tabella e della prima colonna.

Nome: 'group by tabella.nomecampo having 0=0—
Password: qualsiasi
Risultato: fornisce il nome del secondo campo coinvolto nella query.

Nome: Pippo —
Password: qualsiasi
Effetto: Autenticazione come utente Pippo, la parte di query riguardante la password viene ignorata.

Nome: ' or 0=0 –
Password:qualsiasi
Effetto: Autenticazione come primo utente della tabella users.

Nome: ' OR "='
Password: ' OR "='
Effetto: Autenticazione senza credenziali. Nessuna parte della query viene ignorata ma il risultato è sempre positivo.

Nome: ' ; drop table members—
Password: qualsiasi
Effetto: Eliminazione completa della tabella.

Nome: ' ;EXEC master..xp_cmdshell 'dir';--
Password: Qualsiasi
Effetto: Apre una sessione di MS SQL server che ottienee un listato della directory.

400.000 HOTSPOT WI-FI

Nata qualche tempo fa come iniziativa di volontariato, la community FON si è trasformata ed è cresciuta fino a superare il milione di iscritti

L'idea di base è semplice: se tutti condividiamo la connessione a Internet di casa tramite Wi-Fi, una volta fuori casa è facile trovare una rete a cui collegarsi. La community FON è nata proprio da questa considerazione, da questo scambio di favori: io creo un hotspot a cui gli altri membri della community si possono collegare e, a mia volta, mi collego agli hotspot che altri mettono a disposizione. Cresciuta notevolmente nel corso degli anni fino a superare i 400.000 hotspot e il milione di iscritti in tutto il mondo, FON si è ben presto trasformata da community a una vera e propria azienda che, tuttavia, affonda ancora le sue basi nella condivisione volontaria. In Italia il suo successo è stato purtroppo inferiore alle aspettative, complice una normativa decisamente complessa e la confusione che molti fanno tra un hotspot FON e una rete wireless aperta. Quest'ultima è severamente vietata perché non permette l'identificazione degli utilizzatori e comporta un'infrazione alle leggi antiterrorismo. Per l'uso di un hotspot FON, invece, occorre identificarsi e la community è in grado di risalire alla vera identità dell'utente, sia per accertarsi che sia membro della community, sia per identificare il suo grado. FON era partita come una comunità di utenti alla pari ma è da qualche anno che un utente può avere gradi diversi di partecipazione. Ci sono utenti FON che si limitano a condividere la filosofia di base e possono navigare gratuitamente da qualsiasi hotspot in cambio della condivisione della loro connessione casalinga. Chi non ha una connessione da condividere può acquistare credito e navigare sugli hotspot FON a prezzi convenienti. Altri invece, come gestori di bar e ristoranti, condividono la loro connessione creando hotspot FON ma rinunciano al diritto di usare la rete FON in cambio di una percentuale sul guadagno generato dagli utenti paganti. Il meccanismo, visti gli anni di rodaggio, sembra funzionare bene: FON è attualmente la rete di hotspot Wi-Fi più diffusa al mondo, complice anche la creazione di router creati su misura per questo sistema e gestiti completamente da remoto. Malgrado gli evidenti lati positivi, tuttavia, occorre registrare che queste cifre non sono completamente veritiere: sullo stesso sito di FON sono disponibili mappe utili per trovare facilmente gli hotspot e che permettono di impostare filtri di selezione. Eliminando dalle mappe gli hotspot che non hanno dato segnali di vita nell'ora precedente, il numero dei punti di accesso disponibili cala drasticamente. Malgrado questo limite, la tecnologia c'è, è diffusa e l'offerta resta comunque molto ampia.

La fonera è il router, venduto da FON per la creazione degli Hotspot. Costa poco, funziona bene e prevede sia un canale privato che uno pubblico, da condividere.

PROGRAMMI INUTILI

Accendere per la prima volta un computer è un po' come dormire la prima volta in una casa nuova. Solo che, in questo caso, alcune cose non funzionano come dovrebbero

Compriamo un computer nuovo, apriamo con impazienza la confezione, facciamo tutti i collegamenti del caso, lo accendiamo ed eccolo lì: un sistema operativo pulito, pronto per accogliere i nostri programmi, per soddisfare le nostre necessità. Invece no: se i puristi amerebbero poter scegliere se avere o meno il sistema operativo OEM, a molti altri piace che questo sistema sia già installato e pronto per lavorare. La sorpresa, però, riguarda tutti e va ben oltre il sistema operativo. In aggiunta al solito Windows, sulla quasi totalità dei computer preinstallati, ci sono una serie di link, programmi, utility e stupidaggini varie di cui quasi tutti possono fare a meno.

::Un computer sporco

Per la maggior parte si tratta di versioni di prova di vari programmi. Altre volte si tratta di versioni complete di cose completamente inutili. Gli esempi si sprecano e sui computer nuovi si trova proprio di tutto. In cambio della possibilità di mettere su tutti i computer venduti la versione completa di Microsoft Works, per esempio, su moltissimi computer si trova la versione di prova di Microsoft Office 2007. Il primo programma è completamente inutile perché, sostanzialmente, inutilizzato dalla maggior parte degli utenti: troppo limitato per alcune persone, troppo complesso per altre, la versione ridotta di Office viene ampiamente superata dalle alternative gratuite, come OpenOffice, risultando solo un programma che occupa spazio su disco inutilmente. Quanto alla versione di prova di Office 2007 c'è poco da dire: il suo uso è limitato nel tempo e non è nemmeno molto diffuso. Serve a ben poco. Un altro esempio? Gli antivirus. Molti rivenditori

obbligano a scegliere di installare insieme al sistema OEM anche un antivirus a scelta tra McAfee o Norton, ovviamente con abbonamento ridottissimo della validità di un mese. Rispetto ad altri produttori, che non permettono di scegliere, è un passo avanti ma nel complesso è un'operazione inutile: in ambito casalingo ci sono validissime alternative gratuite, come il professionale Avast! Antivirus, mentre in ambito aziendale si usa l'antivirus (e l'abbonamento) acquistati dall'azienda. Perché obbligare gli utenti, specialmente inesperti, a configurare sistemi di protezione che non gli interessano?

Microsoft è stata la prima a stringere accordi con i produttori per la distribuzione di proprio software, specialmente per i sistemi operativi.

Perché costringere gli utenti a darsi da fare per ripulire il proprio computer, nuovo, da questi fastidiosi programmi? Le cose non migliorano certo pensando alle utility del produttore dell'hardware: se alcune risultano molto utili, altre sono del tutto inutili o, addirittura, dannose. Pensiamo all'elenco di link già pronti nel browser che rimandano ai vari siti del produttore del PC ma anche alle utility per controllare in modo semplificato la rete wireless o mantenere le password. Tutte cose che, se non esplicitamente necessarie, occupano inutilmente la memoria.

::Pulizia!

Il primo passo a cui un utente è costretto quando accende il nuovo PC è spesso quello di iniziare la disinstallazione di tutti questi inutili software. Scoprendo, in molti casi, che possono arrivare ad occupare diversi preziosissimi GB sul disco. Molti utenti, però, si limitano ad ignorare il software preinstallato, abbandonandolo. In altri casi, specialmente per gli antivirus o i programmi di sicurezza, gli utenti accettano di seguire il wizard di configurazione iniziale. Il risultato è che le aziende che hanno spinto l'inserimento del software in questione ottengono, in molti casi, un abbonato in più: un utente che si rassegna a pagare perché non sa come togliersi di torno un antivirus che continua a ricordargli che è scaduto. A questo proposito occorre segnalare che è piuttosto facile ritrovarsi utenti falsamente sicuri: hanno l'antivirus, quindi sono tranquilli, ma la mancata sottoscrizione comporta il mancato aggiornamento, con danni enormi per la sicurezza. Anche decidendo di disinsta llare questi programmi dopo un mese, posto di riuscirci, occorre notare come la maggior parte di questi software è piuttosto invasiva con il sistema ed alcune loro parti giacciono sul disco, inutilizzate, fino alla riformattazione. A proposito di riformattazione occorre notare come anche questa operazione non permetta di togliersi di torno questi sgradevoli ospiti. Nella maggior parte dei casi, il disco o la partizione di ripristino del computer sono personalizzati dal produttore con gli stessi identici programmi. Quindi si può arrivare al paradosso per cui si ripristina il computer che ha problemi e ci si ritrova con programmi che si sperava di non rivedere più.

Dell ci obbliga a scegliere se installare Office. Ma se ci piacesse Open Office? Perché acquistare un software che non vogliamo?

I computer HP di distinguono per l'ottimo rapporto prezzo/prestazioni... e per un mucchio di inutile software preinstallato.

Gli abbonati all'antivirus McAfee, come per il concorrente Norton, sono soprattutto gli utenti che se lo ritrovano preinstallato.

::A chi conviene?

Questa politica di distribuzione è caldeggiata da molti produttori di software con la scusa di fornire agli utenti una serie di strumenti utili. L'antivirus per proteggere il PC, il programma d'ufficio per iniziare subito a lavorare e così via. Nella realtà, questa è soltanto, appunto, una scusa. Lo scopo, evidente, è quello di far affezionare gli utenti meno esperti a prodotti che non si riesce a spingere in altro modo. Il vantaggio di un'operazione del genere sembra essere solo quello di permettere ai produttori di PC di guadagnare qualche soldo dagli accordi commerciali per la distribuzione di questi software oppure di ottenere sconti per gli acquisti. Purtroppo, l'abitudine di prendere in giro gli utenti offrendogli servizi non richiesti non è destinata a esaurirsi presto. Microsoft, proprio grazie a questa strategia, domina ancora il mercato dei sistemi operativi. La sua applicazione ad altri software, sia da parte della stessa Microsoft che da parte di altri produttori, non fa altro che svelare il tentativo di mantenere quote di mercato di fronte all'avanzata inarrestabile del software Open Source.

Sfidiamo altri hacker in un gioco di bravura

CREIAMO UNA HACKING CHALLENGE

Negli ultimi anni è notevolmente aumentato il numero di hacking challenge su Internet. Questi siti consistono solitamente di una serie di indovinelli o puzzle, proposti in ordine di difficoltà crescente; risolvendone uno è possibile guadagnare punti o avanzare verso livelli successivi che consentono di accedere a un numero maggiore di risorse. Indovinelli e puzzle, naturalmente, sono creati "a misura di hacker": le conoscenze richieste per partecipare coprono infatti tutto lo scibile informatico, dai linguaggi di scripting alla crittografia, dal reverse engineering alle tecniche di ricerca su Internet. Partecipare a queste gare è particolarmente interessante poiché non solo è istruttivo, ma ci permette anche di entrare in contatto con gruppi di persone che condividono i nostri interessi. E poi un po' di narcisismo non fa mai male: ogni hacking challenge che si rispetti, infatti, ha anche una "hall of fame", all'interno della quale si trovano i nomi degli hacker che hanno totalizzato il punteggio più alto.

:: Proponiamo nuovi indovinelli

Se da un lato partecipare a una hacking challenge come giocatore è molto divertente, far giocare altre persone può esserlo ancora di più. Improvvisarsi "riddlers" (cioè creatori di indovinelli) non è particolarmente complicato dal punto di vista tecnico: tutto ciò che serve è un po' di tempo, insieme a una buona dose di creatività. L'idea alla base di tutto è che la risposta finale a un indovinello possa sempre essere riassunta in una semplice stringa di testo: nel caso più semplice un nome, fino ad arrivare a sequenze più o meno lunghe di caratteri apparentemente casuali. Il modo più semplice per verificare questa stringa è usarla come parte dell'URL della pagina contenente l'indovinello successivo, richiedendo all'utente di collegarsi manualmente a questa pagina oppure usando del codice Javascript per generare automaticamente il nuovo indirizzo Web: se la risposta è giusta verrà caricata la pagina corretta, in caso contrario il server Web restituirà un messaggio di errore.

:: Gli strumenti

Qualsiasi sia la nostra scelta, non dovremmo avere grosse difficoltà a trovare in Internet lo spazio e il software necessario per creare la nostra hacking challenge. Possiamo anche creare un ambiente di test in locale sul nostro computer, utilizzando pacchetti LAMP (Linux+Apache+PHP+MySQL) già pronti. Ad esempio, XAMPP (http://www.apachefriends.org/it/xampp.html) è una distribuzione Apache che contiene al suo interno anche PHP, MySQL e Perl: l'installazione

Il sito ascii-table.com mette a disposizione una tabella ASCII con codici in decimale, esadecimale, ottale e binario, insieme a una collezione di convertitori di testo in diversi formati.

è studiata per essere il più semplice possibile e in pochi minuti possiamo cominciare a fare esperimenti sul nostro sito.

:: Troviamo ispirazione

Prima di inventare dei nuovi indovinelli ci converrà documentarci per bene, verificando cosa è già stato fatto e cosa in generale piace di più. Per aiutarci nella scelta, anziché utilizzare dei motori di ricerca, ci conviene partire da alcuni siti specializzati. Per esempio Hackergames.net (http://www.hackergames.net) è un portale storico per questo genere, che raccoglie i link a quasi 150 challenge differenti: per ognuna di esse vengono mostrati la lingua, una descrizione e una serie di review scritte dagli stessi utenti.

:: Psicologia hacker

L'unica regola in una hacking challenge è che non ci sono regole: se la soluzione a un nostro indovinello non è quella che avevamo previsto, tanto meglio: significa che chi l'ha trovata ha più fantasia di noi! Cercare strade "alternative" è un approccio comune per un hacker, quindi non dobbiamo stupirci se per trovare le soluzioni degli indovinelli vengono sfruttate le vulnerabilità del nostro sistema. Ecco, quindi, alcuni consigli per mantenere la nostra sfida il più divertente possibile (per i giocatori ma anche per noi): verifichiamo la sicurezza dei nostri script,

We Chall mostra, per ogni utente, un grafico con i progressi fatti in ogni sito a cui è iscritto.

in particolare contro gli attacchi più frequenti (come ad esempio SQL injection, se salviamo i dati all'interno di un database). Non affidiamoci alla "security by obscurity", basando cioè la sicurezza del nostro sito sulla segretezza di alcune informazioni: diamo per scontato che queste prima o poi possano essere scoperte e agiamo di conseguenza. Ad esempio, non conserviamo le soluzioni agli indovinelli in chiaro ma cifriamole, in modo che chi le trova debba sudare ancora un po' prima di poter passare al livello successivo; uno dei metodi più stupidi, ma allo stesso tempo efficaci in caso di password brevi, è il bruteforce: usiamo stringhe segrete lunghe e difficili da trovare usando questo sistema e chiariamolo da subito; se ce la caviamo con la programmazione possiamo lasciare intenzionalmente alcuni "buchi" nel sistema che possono essere sfruttati per abilitare nuove feature all'interno del sito, come ad esempio un forum segreto oppure un elenco di risorse nascoste. Se riceviamo un messaggio da qualcuno che ci avverte di una vulnerabilità, consideriamolo un contributo costruttivo. Cerchiamo di scoprirne di più, correggiamo il baco e documentiamo il tutto in modo che anche gli altri utenti possano imparare qualcosa dal nostro errore e dall'abilità di chi l'ha scoperto. Infine, sfidiamo tutti quanti a trovarne altri: questo renderà la sfida molto più interessante...

XAMPP è il sistema più rapido per attivare un server LAMP sul proprio computer Windows, Linux o Mac.

Chiavette che non navigano, download interminabili, connessioni che saltano. È inutile: il wireless non è una cosa seria

Internet wireless

Secondo i suoi promotori, dovrebbe stare in una vetrinetta all'ingresso di casa. Secondo altri non serve a nulla. Per altri ancora è indispensabile mentre alcuni pensano che l'acquisto sia stato un errore. Ovviamente stiamo parlando della Vodafone Station: l'apparecchio miracoloso che promette di sganciarci dai cavi telefonici e dal giogo del canone Telecom. Ma si parla sempre più anche delle chiavette USB per collegarsi a Internet: con la scusa di avere spesso un traffico a consumo, si stanno diffondendo molto rapidamente. Sembra quasi che sia ormai indispensabile avere la possibilità di collegarsi a Internet con il proprio computer dovunque, in ogni momento, anche se non ci si sposta mai da casa o se si usa la connessione soltanto una volta alla settimana.

:: Roba vecchia

La possibilità di collegarsi a Internet tramite la rete cellulare, però, non è certo una novità recente. Questa tecnica è diffusa da diversi anni, soprattutto in ambito professionale. A cambiare è stata senz'altro al tecnologia: l'UMTS e dell'HSDPA hanno aumentato la banda disponibile per i collegamenti, permettendo l'arrivo sui cellulari di siti Web reali e non delle versioni ridotte e poco funzionali tipiche dei collegamenti di qualche anno fa. Questo ha dato modo ai produttori di cellulari di integrare nei loro apparecchi dei veri e propri browser. Limitati rispetto a quelli tradizionali ma comunque capaci di offrire una fruizione più completa del Web e di tutte le tecnologie correlate. Questo progresso ha permesso la netta diminuzione dei costi e la sostanziale trasformazione di questo modo di connettersi. Qualche anno fa, stabilire una connessione alla rete cellulare era un'operazione per addetti ai lavori che richiedeva cellulari molto costosi ed aveva tariffe degne del miglior champagne. Oggi l'operazione è nettamente più semplice, la stragrande maggioranza dei cellulari si collega a Internet con pochi passaggi e le tariffe sono diminuite moltissimo. Non è tutto rose e fiori però: per alcuni versi la situazione è peggiore di quella passata perché manca informazione. Le pubblicità di questi collegamenti, infatti, segnalano velocità paragonabili a quelle delle migliori ADSL, che attualmente arrivano a 7,2 Mb al secondo. Indicazioni riportate molto visibilmente, al punto di far sognare chi ancora non dispone di centraline telefoniche adatte all'ADSL. L'indicazione

che questa velocità è la massima teorica raggiungibile viene demandata a minuscole note informative, mentre il fatto che si sta parlando di megabit e non di megabyte (multiplo dell'unità di misura delle dimensioni dei file a cui siamo tutti abituati) viene lasciato alla libera conoscenza dell'utente.

::Velocità basse

Nella realtà, come per l'ADSL, la velocità reale dipende dalle condizioni di traffico sulla rete dell'operatore e difficilmente si riescono a raggiungere buoni risultati. Diversamente dall'ADSL, inoltre, con i collegamenti UMTS/HSDPA le cose si complicano ulteriormente perché la velocità diminuisce anche se ci sono molti utenti collegati alla nostra stessa cella radio, oppure se la nostra ricezione non è perfetta. A peggiorare ulteriormente le cose c'è il fatto che nessun operatore propone una vera connessione a costo flat: nel migliore dei casi si paga un canone di qualche decina di euro al mese per poter scaricare, se va bene, qualche giga al mese. Un traffico bassissimo se si desidera sfruttare la condivisione dei file. Un'offerta assolutamente non paragonabile con quella delle ADSL classiche che, alla fine, permettono un traffico illimitato. Ulteriore complicazione all'interno del mercato riguarda gli abbonamenti orari: quasi come se si trattasse di una corsa, tutti gli operatori vendono chiavette USB che includono tariffazioni basate sul tempo passato online. Una vera e propria presa in giro visto che il tempo di connessione, contrariamente al traffico, non incide sui costi dell'operatore e che questo genere di connessione costringe gli utenti a improbabili navigazioni cronometrate. Allo stato attuale, forse, l'attesa sembra essere ancora la strategia più saggia. L'attuale mercato non potrà mantenere i costi, soprattutto quelli nascosti, sui livelli attuali e gli operatori dovranno espandere le loro infrastrutture se vorranno conquistare nuove quote. Per ora, quindi, è consigliabile ricorrere a queste tecnologie solo se veramente indispensabili e, in ogni caso, di evitare accuratamente gli abbonamenti a tempo o a consumo in favore di quelli semi-flat.

UNA STATION IN TASCA

Prendiamo un router, aggiungiamo un modem ADSL, un access point, una chiavetta UMTS/HDSPA per il collegamento a Internet, un piccolo server Samba e il supporto al VoIP. Mescoliamo il tutto e otterremo una Vodafone Station: l'accessorio tanto reclamizzato da Vodafone che promette di portare Internet anche in zone non coperte dall'ADSL. Questo accessorio, nato per sganciare le utenze dal giogo di Telecom, si sta diffondendo moltissimo ma diverse persone non si rendono conto che ce l'hanno già... In tasca! Basta pensarci: la maggior parte degli smartphone dispone di un collegamento Wi-Fi per usare Internet a casa senza aumentare spese telefoniche. In caso di mancata copertura Wi-Fi, invece, possono collegarsi alla Rete usando l'UMTS o l'HDSPA della rete cellulare. Se si riuscisse a usare le funzioni Wi-Fi per renderle equivalenti a quelle di un normale router Wi-Fi e a far transitare il traffico wireless sulla rete cellulare, si disporrebbe di una specie di Vodafone Station portatile da usare ovunque, non per avere Internet su un singolo computer ma su un insieme: una specie di Personal Wi-LAN da sfoderare quando, magari, si va a casa di amici o si viaggia per lavoro in zone non coperte dall'ADSL. Il bello della cosa è che la trasformazione di uno smartphone in un sistema del genere è quasi banale: basta avere il programma giusto. Il sistema Wi-Fi, per sua natura, non è vincolato a un ruolo specifico: una scheda di ricezione può diventare una specie di access point dalle capacità ridotte rispetto a un AP dedicato. Così, la scheda Wi-Fi nello smartphone può facilmente essere trasformata nel sistema di connessione di un piccolo AP. Allo stesso modo, il traffico generato direttamente dal cellulare o da connessioni tra questo ed altri sistemi è indistinguibile agli operatori perché smartphone lo gestisce autonomamente: che il traffico derivi dallo scaricamento di un file direttamente sul cellulare oppure dal suo collegamento bluetooth con un computer, all'operatore non interessa. Questo ci rende liberi di agire sul cellulare, modificando il suo sistema di funzionamento e permettendo un flusso di dati normalmente non ammesso. La prima e unica cosa da fare è quella di installare il programma adatto al nostro sistema operativo. Se usiamo uno smartphone basato su Windows Mobile possiamo provare WM WiFi Router, www.wmwifirouter.com: costa poco più di 20 euro IVA inclusa. Con altri sistemi, come Symbian, possiamo rivolgerci a prodotti come Joiku Spot Lite (gratuito ma con alcune limitazioni) oppure Joku Spot Premium, www.joikuspot.com.
Ovviamente le caratteristiche del nostro router Wi-Fi su rete cellulare dipenderanno dall'hardware disponibile. WM WiFi Router installato su uno smartphone capace di raggiungere i 7 Mbps potrà arrivare a quella velocità. Su smartphone meno evoluti avrà una velocità più limitata, ma volete mettere con la possibilità di estrarre il telefono dalla tasca, avviare il programma e fornire Internet tramite Wi-Fi agli amici in una zona dove non c'è ADSL?

Pochi sanno che l'equivalente della Vodafone Station è già a portata di mano: qualsiasi telefono cellulare di ultima generazione può sostituirla.

OFFICE 2007 & LINUX: si può fare!

Qualcuno storcerà il naso, ma Linux va oltre le guerre di religione e regala ogni giorno nuove sorprese

E' possibile far girare Microsoft Office 2007 su una distribuzione di Linux. Ai puristi non piacerà affatto, l'operazione non è garantita al 100% e per realizzare questo hacking si devono emulare molte funzioni di Windows (la procedura prevede alcune pre-installazioni) per offrire all'installer di Office l'ambiente corretto nel quale installare le varie applicazioni. Inoltre l'infrastruttura di base è tuttora in beta, il che può dar vita a qualche problema. Ma si può fare.

:: Come è possibile

L'idea di questo progetto è nata all'interno della community di Wine, il software che offre ad applicazioni Windows un substrato compatibile (ovvero non un emulatore e da qui il suo nome ricorsivo: Wine Is Not an Emulator) che sfrutta le potenzialità di Linux per farle funzionare. Lo stesso Wine è tuttora in sviluppo e data la mole di informazioni non documentate ufficialmente da Microsoft, il compito è quasi improbo.

Tuttavia sono molti i casi di successo e tra questi c'è Microsoft Office. Se si legge la pagina del wiki relativo a questo progetto (appdb.winehq.org/objectManager.php?sClass=version&iId=4992) si scopre che le possibilità di riuscire sono basse (un 33%), ma ci sono e sono documentati i casi positivi per i quali viene indicata la distribuzione utilizzata e la versione di Wine.

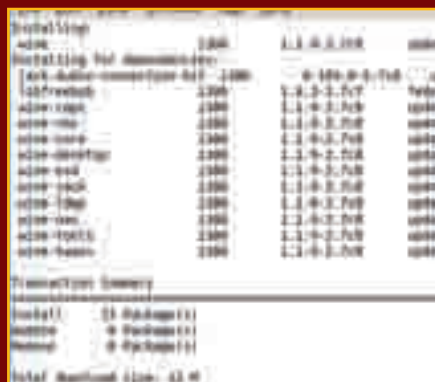
In particolare, le recenti versioni (a partire dalla 1.1.17) hanno compromesso il buon funzionamento dell'in-

staller di Office 2007 e di conseguenza non si possono utilizzare le distribuzioni che vengono proposte con Wine 1.1.19, a meno di non procedere a un downgrade dell'applicazione.Abbiamo infatti provato con esiti negativi Ubuntu 8.04 LTS, Ubuntu/Kubuntu/Xubuntu 8.10, nonostante fossero riportati con status platinum, gold, bronze proprio perché la versione di Wine era appunto precedente a quella rilasciata.

Per evitare quindi macchinose riconfigurazioni, abbiamo cercato direttamente una distribuzione leggermente più datata come Fedora 8 che veniva indicata come idonea a far funzionare l'installer. Di base questa distribuzione viene fornita con la versione 1.1.7 che su aggiornamento (yum update) la sincronizza alla 1.1.9 giudicata più stabile. L'installer di Office è garantito come funzionante fino alla versione 1.1.16, quindi siamo nella condizione giusta.

:: La procedura

Ovviamente occorre avere un cd originale di Office 2007 (in una delle sue diverse versioni) per fare le prove e almeno 2GB liberi una volta installata la distribuzione (sconsigliamo di usare una macchina virtuale date le richieste di risorse della suite di Microsoft). Questo perché è suggerito di installarlo completamente, perché l'installazione personalizzata (custom) non è ancora garantita. Wine ma non fornisce tutto il supporto richiesto da un'applicazione pesantemente integrata nel sistema operativo come Office 2007; va quindi seguita una procedura di preparazione che consta di pre-installazioni.

Assicuriamoci che la distribuzione sia connessa a Internet, configurando opportunamente una scheda di rete. Va poi verificato che sia installata la versione corretta di Wine, per quanto già anticipato. Se il pacchetto è già installato in una finestra terminale è possibile lanciare winecfg, altrimenti dobbiamo aggiungerlo. Su Fedora diamo il comando "yum install wine", su Debian/Ubuntu "apt-get install wine" e attendiamo la corretta installazione. Al termine verifichiamo la versione installata con il comando "wine -version".

Su Fedora 8 si può anche aggiornare la distribuzione in modo da avere Wine 1.1.9.

Ora possiamo configurare Wine tramite "winecfg". In questa fase indicheremo solamente la versione da emulare (è consigliato Vista) in Applications e agganciamo in Drives/media/cdrom0 al drive D: (cliccando su Autodetect e poi su Add).

Impostiamo in questa fase la versione di Windows su Vista, più tardi imposteremo XP.

Ora occorre uno script geniale chiamato winetricks (www.kegel.com/wine/winetricks) che si occuperà del "lavoro sporco" di riconfigurare l'ambiente Linux in qualcosa che appaia agli occhi dell'installer il più simile possibile a Windows. Una volta scaricato daremo infatti il comando "sh winetricks msxml3 dotnet20 gdiplus riched20 riched30 vcrun2005sp1 " che scaricherà dal sito della Microsoft diverse patch e librerie che verranno correttamente gestite da wine (Microsoft XML Parser, Microsoft .NET Framework 2.0, Microsoft PowerPoint Viewer 2003, Microsoft Visual C++ 2005 SP1). Scarichiamo dall'indirizzo www.mediafire.com/?njtut9aswdk una versione modificata di rpcrt4.dll che andremo a sostituire in "~/.wine/drive_c/Windows/system32/" rinominando quella presente in .bak (ci occorrerà più avanti quella originale). Apriamo nuovamente winecfg e in Libraries aggiungiamo rpcrt.

:: Lanciamo Office!

Siamo pronti per lanciare il programma di installazione di Office: inseriamo il CD e in /media/cdrom0 potremo lanciare il setup (a seconda della distribuzione potrebbe essere necessario lanciare "wine setup.exe" da terminale). Una volta partito il programma clicchiamo su Install Now e aspettiamo che completi la procedura.

Una volta partito l'installer eseguiamo il setup completo di tutta la suite.

Ultimo passo prima di godercelo è quello di ripristinare la dll corretta in "~/.wine/drive_c/Windows/system32" con il comando "mv rpcrt4.bak rpcrt4.dll". Torniamo poi in winecfg eliminiamo in Libraries rpcrt e selezioniamo per Windows la versione XP.

Se tutto è filato liscio avremo in Applications->Wine->Programs->Microsoft Office tutti i programmi della suite di Office più usata al mondo.

Massimiliano Brasile

Mobile Wardriving

Come usare il nostro smartphone per catturare reti wi-fi

Per effettuare un test di rilevamento delle WLAN non è più necessario avere a disposizione un notebook, perché si può avere tutto concentrato su un dispositivo molto più piccolo e in grado di passare inosservato: un telefonino con sistema operativo Symbian 3a versione con Wi-Fi integrato.

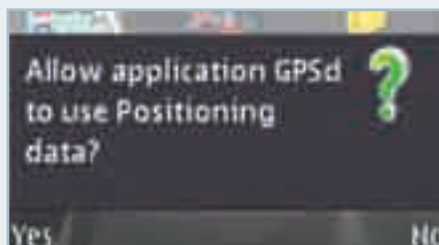
:: Cosa occorre

L'hardware è di primo livello, ma occorre il software adatto. Fortunatamente è stato effettuato un porting di librerie open source dedicate allo sniffing su Symbian che sono state inserite in Barbelo, un simpatico tool che si installa senza problemi sul nostro Nokia (soprattutto se abbiamo già provveduto a sbloccarlo come descritto in HJ 174) che possiamo scaricare da HYPERLINK http://darkircop.org/barbelo (divertenti le note annidate nel codice html della home-page, che fanno pensare che il team sia italiano). Il software è ancora nei primi stadi di sviluppo (l'ultima versione disponibile al momento è la 0.3), ma permette di avere le funzionalità di monitoraggio presenti in strumenti più maturi come Kismet o Netstumbler, adattate allo schermo e all'interfaccia di un telefonino, con in più la possibilità di esportare i dati raccolti in XML nel formato di Kismet.

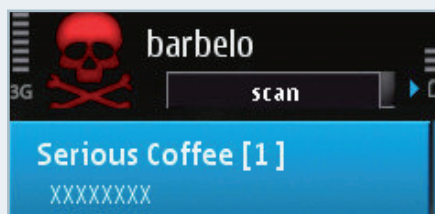
Componente opzionale, ma decisamente utile se si vuole testare un'area intera, è il monitor gps GPSd (scaricabile allo stesso link di Barbelo; ultima versione disponibile al momento la 0.2): grazie al "demone", con l'aggiunta di un'antenna gps possiamo attivare il tracking dei nostri monitoraggi che verranno inclusi nei log che Barbelo è in grado di realizzare.

Installiamo i due SIS: accendiamo l'antenna GPS e lanciamo GPSd; una volta avviato lanciamo Barbelo.

:: Avviamo il test

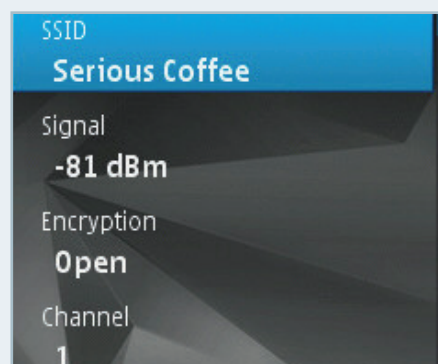
Lanciando GPSd, il software chiederà accesso ai dati di posizionamento (GPS), per leggere la posizione, al network per comunicare con Barbelo e successivamente alla connessione bluetooth nel caso non trovi un'antenna integrata e si sia costretti a usarne una esterna.

Confermiamo a GPSd che può accedere ai dati GPS e che può attivare la connessione dati.

Lasciamo che il demone si autentichi e una volta fissato il segnale visualizzeremo le coordinate catturate dall'antenna (indicando valori diversi da zero nei campi Latitude/Longitude).
Ora premiamo su **hide** per lasciarlo in background e lanciamo Barbelo. Siamo pronti.L'interfaccia di Barbelo è semplice, ma estremamente ben organizzata. La prima schermata presenta l'elenco delle reti Wi-Fi che trova (ed è sempre sorprendente scoprire quante reti ci sono attorno a noi quasi ovunque ormai) e per ciascuna visualizza il SSID, se trasmesso, la forza del segnale (tramite un semplice istogramma di X) e una sintesi della protezione applicata. Come già confermato in passato, molte reti rilevate durante le prove utilizzano il protocollo WEP, ma inizia ad essere apprezzabile il numero di reti che utilizzano quello WPA.
Se scorriamo con i tasti del menu le varie schermate possiamo spostarci nella pagina dedicata alla mappa (che avrà informazioni utili solo se stiamo usando il demone GPS, altrimenti vedremo solo un puntino in mezzo allo schermo) e una finestra di debug dove per ora viene solamente visualizzato lo stato della connessione GPS (connected o non-connected). Nel caso non ci sia connessione il puntino è rosso, in caso contrario vediamo un bel puntino verde.

A seconda della rapidità dell'antenna dovremo aspettare più o meno tempo per fissare il segnale.

Nella pagina scan vediamo tutte le reti rilevate e la potenza del segnale.

:: La mappatura delle reti

A dire il vero la mappa è davvero spartana e non c'è al momento la possibilità di caricare uno sfondo legato al territorio o altre possibilità che sarebbero interessanti, ma speriamo che gli sviluppatori ci possano lavorare. Se Barbelo riceve i dati, integra alle sue informazioni la posizione rilevata ed è possibile registrare tutto nei log selezionando **Start Log** dal menu. Con un po' di pazienza sarà possibile ricostruire il percorso su una mappa reale e collocare le reti. Se proviamo a switchare su GPSd noteremo che ora è indicata la presenza di un client che sta utilizzando i dati raccolti. Torniamo ora nella schermata principale di Barbelo. Se clicchiamo su una delle reti rilevate possiamo leggere tutti i dati trasmessi dall'access point e in particolare: la potenza del segnale in dBm, l'esatta protezione applicata, il canale Wi-Fi utilizzato, la modalità (ad hoc, infrastructure), il BSSID, le coordinate GPS registrate nell'istante in cui il segnale è stato rilevato, i dati temporali tra il primo e l'ultimo rilevamento. Queste informazioni, unite sempre a molta pazienza, ci permetteranno di identificare con maggior precisione l'origine del segnale verificando l'aumento della potenza e a seconda dei casi anche l'aumento dei messaggi rilevati dalla nostra antenna Wi-Fi.

Quando abbiamo le informazioni GPS e ci interessa registrare i dati avviamo il log.

Scheda riepilogativa della rete rilevata da scorrere per vedere tutte le informazioni.

Spostiamoci mentre il software sta raccogliendo i dati, così da avere dei log interessanti e quando abbiamo finito, nel menu Opzioni selezioniamo **Stop Log** e chiudiamo Barbelo (**Options->Exit**). Una volta trasferiti i log sul PC possiamo passare all'analisi e alla loro elaborazione. Il formato è lo stesso usato da Kismet e grazie a uno script in perl possiamo utilizzare Google Earth per visualizzarli. Lo script si chiama Kisgearth.pl (**code.google.com/p/kisgearth**) e da Linux basta dare il comando: **./kisgearth.pl -oN Barbelo-MMM-DD-YYYY-1.kml -n1 — Barbelo-MMM-DD-YYYY-1.xml** per convertire il singolo file XML. Lo script genererà l'equivalente kml che è il formato usato da Google Earth e che restituirà la mappatura delle reti rilevate sovrapposta alle sue foto satellitari.

NoeXKuzE